Exhibit C

Address Resolution Protocol

From Wikipedia, the free encyclopedia

In computer networking, the **Address Resolution Protocol (ARP)** is the method for finding a host's hardware address when only its IP address is known. Due to the overwhelming prevalence of IPv4 and ethernet, ARP is primarily used to translate ethernet MAC addresses from IP addresses. It can, however, easily be used for IP over ATM or FDDI.

ARP is used in four cases of two hosts communicating:

1. When two hosts are on the same network and one desires to send a packet to the other
2. When two hosts are on different networks and must use a gateway/router to reach the other host
3. When a router needs to forward a packet for one host through another router
4. When a router needs to forward a packet for one host to the destination host on the same network

The first case is used when two hosts are on the same physical network (i.e., they can directly communicate without going through a router). The last three cases are the most used over the internet as two computers on the internet are typically separated by more than 3 hops.

Internet protocol suite

Layer	Protocols
Application	DNS, TLS/SSL, TFTP, FTP, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SNMP, SSH, TELNET, BitTorrent, RTP, rlogin, ENRP, ...
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, ...
Network	IP (IPv4, IPv6), ICMP, IGMP, **ARP**, RARP, ...
Link	Ethernet, Wi-Fi, Token ring, PPP, SLIP, FDDI, ATM, DTM, Frame Relay, SMDS, ...

Imagine computer A sends a packet to computer D and there are two routers, B & C, between them. Case 2 covers A sending to B; case 3 covers B sending to C; and case 4 covers C sending to D.

ARP is defined in RFC 826 (http://www.ietf.org/rfc/rfc826.txt).

Contents

Variants of the ARP protocol

ARP was not originally designed as an IP-only protocol although today it is primarily used to map IP addresses to MAC addresses.

ARP can be used to resolve MAC to many different Layer 3 protocols. ARP has also been adapted to resolve other kinds of Layer 2 addresses; for example, ATMARP is used to resolve ATM NSAP addresses in the

Classical IP over ATM protocol.

ARP Mediation

ARP Mediation refers to the process of resolving Layer 2 addresses when different resolution protocols are used on either circuit, for e.g. ATM on one end and Ethernet on the other.

Inverse ARP

The **Inverse Address Resolution Protocol**, a.k.a. **Inverse ARP** or **InARP**, is a protocol used for obtaining Layer 3 addresses (e.g. IP addresses) of other stations from Layer 2 addresses (e.g. the DLCI in Frame Relay networks). It is primarily used in Frame Relay and ATM networks, where Layer 2 addresses of virtual circuits are sometimes obtained from Layer 2 signalling, and the corresponding Layer 3 addresses must be available before these virtual circuits can be used..

Comparison between ARP and RARP

ARP translates Layer 3 addresses to Layer 2 addresses, therefore InARP can be viewed as its inverse. In addition, InARP is actually implemented as an extension to ARP. The packet formats are the same, only the operation code and the filled fields differ.

RARP, like InARP, also translates Layer 2 addresses to Layer 3 addresses. However, RARP is used to obtain the Layer 3 address of the requesting station itself, while in InARP the requesting station already knows its own Layer 2 and Layer 3 addresses, and it is querying the Layer 3 address of another station. RARP has since been abandoned in favor of BOOTP then DHCP.

Packet structure

The following is the packet structure used for ARP requests and replies. Note that the packet structure shown in the table has SHA, SPA, THA, & TPA as 32-bit words but this is just for convenience — their actual lengths are determined by the hardware & protocol length fields.

Hardware type (HTYPE)	Bits 0 - 7	8 - 15	16 - 31
0	Hardware type (HTYPE)		Protocol type (PTYPE)
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)
64	data link layer protocol is assigned a	Sender hardware address (SHA)	
?		Sender protocol address (SPA)	
?		Target hardware address (THA)	
?		Target protocol address (TPA)	

number used in this field. For example, ethernet is 1.

Protocol type (PTYPE)
: Each protocol is assigned a number used in this field. For example, IPv4 is 0x0800.

Hardware length (HLEN)
: Length in bytes of a hardware address. Ethernet addresses are 6 bytes long.

Protocol length (PLEN)
: Length in bytes of a logical address. IPv4 address are 4 bytes long.

Operation
Specifies the operation the sender is performing: 1 for request, and 2 for reply.
Sender hardware address (SHA)
Hardware address of the sender.
Sender protocol address (SPA)
Protocol address of the sender.
Target hardware address (THA)
Hardware address of the intended receiver. This field is zero on request.
Target protocol address (TPA)
Protocol address of the intended receiver.

Request

+	Bits 0 - 7	8 - 15	16 - 31
0	Hardware type = 1		Protocol type = 0x0800
32	Hardware length = 6	Protocol length = 4	Operation = 1
64	SHA = 0x000958D8		
96	SHA (cont'd) = 0x1122		SPA = 0x0A0A
128	SPA (cont'd) = 0x0A7B		THA = 0x0000
160	THA (cont'd) = 0x00000000		
192	TPA = 0x0A0A0A8C		

If a host with IP address of 10.10.10.123 (0x0A0A0A7B) and MAC address of 00:09:58:D8:11:22 wants to send a packet to another host at 10.10.10.140 (0x0A0A0A8C) but it does not know the MAC address then it must send an ARP request to discover the address. The packet shown shows what would be broadcasted over the local network. If the host 10.10.10.140 is running and available then it would receive the ARP request and send the appropriate reply.

Note that the IP address 10.10.10.123 is in dot-decimal notation and is converted to the hexadecimal form when used on the network (*see IPv4 details*). This is done by converting the four octets into hexadecimal (10 = 0x0A; 123 = 0x7B) to yield 0x0A.0x0A.0x0A.0x7B and then concatenated together to yield 0x0A0A0A7B since the decimals are not used in packets.

Also note that MAC addresses are shown in hexadecimal form and the octets are just simply concatenated together to yield the field value.

Reply

+	Bits 0 - 7	8 - 15	16 - 31
0	Hardware type = 1		Protocol type = 0x0800
32	Hardware length = 6	Protocol length = 4	Operation = 2
64	SHA = 0x000958D8		
96	SHA (cont'd) = 0x33AA		SPA = 0x0A0A
128	SPA (cont'd) = 0x0A8C		THA = 0x0009
160	THA (cont'd) = 0x58D81122		
192	TPA = 0x0A0A0A7B		

Given the scenario from the question, if the

host 10.10.10.140 has a MAC address of 00:09:48:D8:33:AA then it would send the shown reply packet. Note that the sender and target address blocks have been swapped (the sender of the reply is the target of the request; the target of the reply is the sender of the request). Furthermore the host 10.10.10.140 has filled in its MAC address in the sender hardware address.

Any hosts on the same network as these two hosts would also see both the request and reply and they can cache the request result as well, thus saving those hosts from having to perform the same query. This is an advantage of a multiple-access bus like ethernet.

See also

- Proxy ARP
- Reverse ARP (RARP)
- Serial line ARP
- Zeroconf
- ARP spoofing

External links

- ARP Sequence Diagram (pdf) (http://www.eventhelix.com/RealtimeMantra/Networking/Arp.pdf)
- RFC 2390 (http://www.ietf.org/rfc/rfc2390.txt) - Inverse Address Resolution Protocol

This article was originally based on material from the Free On-line Dictionary of Computing, which is licensed under the GFDL.

Retrieved from "http://en.wikipedia.org/wiki/Address_Resolution_Protocol"

Categories: FOLDOC sourced articles | Internet protocols | Internet standards